SAFE

CISO's Toolkit:

Acing Cyber Risk Board Reporting

Executive Summary

Managing cyber risk is imperative for every enterprise and every CISO. This is particularly relevant in today's environment of:

- Increasing threat of AI-driven cyber attacks
- Increasing personal liability for CISOs for data breaches
- Increasing regulatory pressure (e.g. SEC Cyber Rule)

This paper provides you with strategies and best practices to create robust and effective board-level reporting so that your organization can be better equipped to navigate potential threats and prevent material damage.

"Board members need a framing of cyber risks in business language of customer, product, operations, and financial risk. We need to connect the dots simply and specifically on why cybersecurity is pivotal to financial security."

Suja Chandrasekaran

Board Member – American Eagle Outfitters, Cardinal Health, Brenntag SE, Agendia Inc

Former Global CTO, Walmart

Former Senior EVP, Chief Digital and Information Officer, CommonSpirit Health

COMPANIES ON A CYBER RISK JOURNEY WITH US

Introduction

CISO Challenges

According to a survey by Deloitte,

> 30% of CIO and CISO respondents say they do not communicate risk around specific business initiatives to other company leaders, indicating they may not know how to share that information in a constructive way.

Cyber risk board reporting requires careful consideration and precision to effectively communicate the potential vulnerabilities and threats facing the company. CISOs often have to navigate complex technical jargon and communicate it in layman's terms to the board.

The Language Barrier:
Difficult to translate technical metrics and cybersecurity threats to boards in an understandable way

Manual Practices:
The data collection process for board or Executive reporting can be inefficient, error-prone, and inconsistent

Compliance-Led Focus:
Current reporting methods often prioritize adherence to regulations over addressing potential threats to the business

Point-In-Time Solutions:
Point-in-time solutions provide fragmented and piecemeal view of cyber risk

Deloitte, 2018: CEO and board risk management survey

1. The Language Barrier

While CEOs and boards are increasingly involved in cybersecurity, major hurdles still hinder effective oversight of cybersecurity risk. One of the primary difficulties arises from the highly technical nature of cybersecurity, which creates a language barrier. Often, CISOs find it challenging to translate present technical metrics and convey cybersecurity concepts in a way that allows boards to grasp the actual risk faced by the organization and the financial implications of incremental cybersecurity investments.

2. Compliance-Led Focus

Current reporting practices tend to focus on activities and projects being worked on rather than prioritizing the business's top risks. While providing valuable information on adherence to security regulations, this compliance-focused reporting method fails to adequately address the potential threats that could severely impact business operations. As a result, identifying the top risks that pose a significant threat to the business may not receive enough attention. Ultimately, the board needs to stay abreast of the most significant exposures to comply with regulations and secure the organization's future.

3. Manual Practices

The manual data collection process for board or Executive reporting can lead to inefficiencies, errors, and potential inconsistencies in the data presented to the board and executives. This process can also result in inaccuracies and mistakes that may affect the overall credibility of the information provided. Furthermore, these inaccuracies could adversely impact the board minutes, which serve as a record of the discussions and decisions.

4. Point-In-Time Solutions

Existing legacy solutions are often point-in-time and can find vulnerabilities quickly, but they fail to provide a complete holistic risk view. It’s not unusual for CISOs to find themselves in a rush to prepare a Cyber Risk Report for a quarterly board meeting. However, the picture painted by such a report is not reflective of the true organization risks, often leading CISOs to present fragmented, piecemeal risk views.

A Recipe for Success to Ace the Next Board Reporting

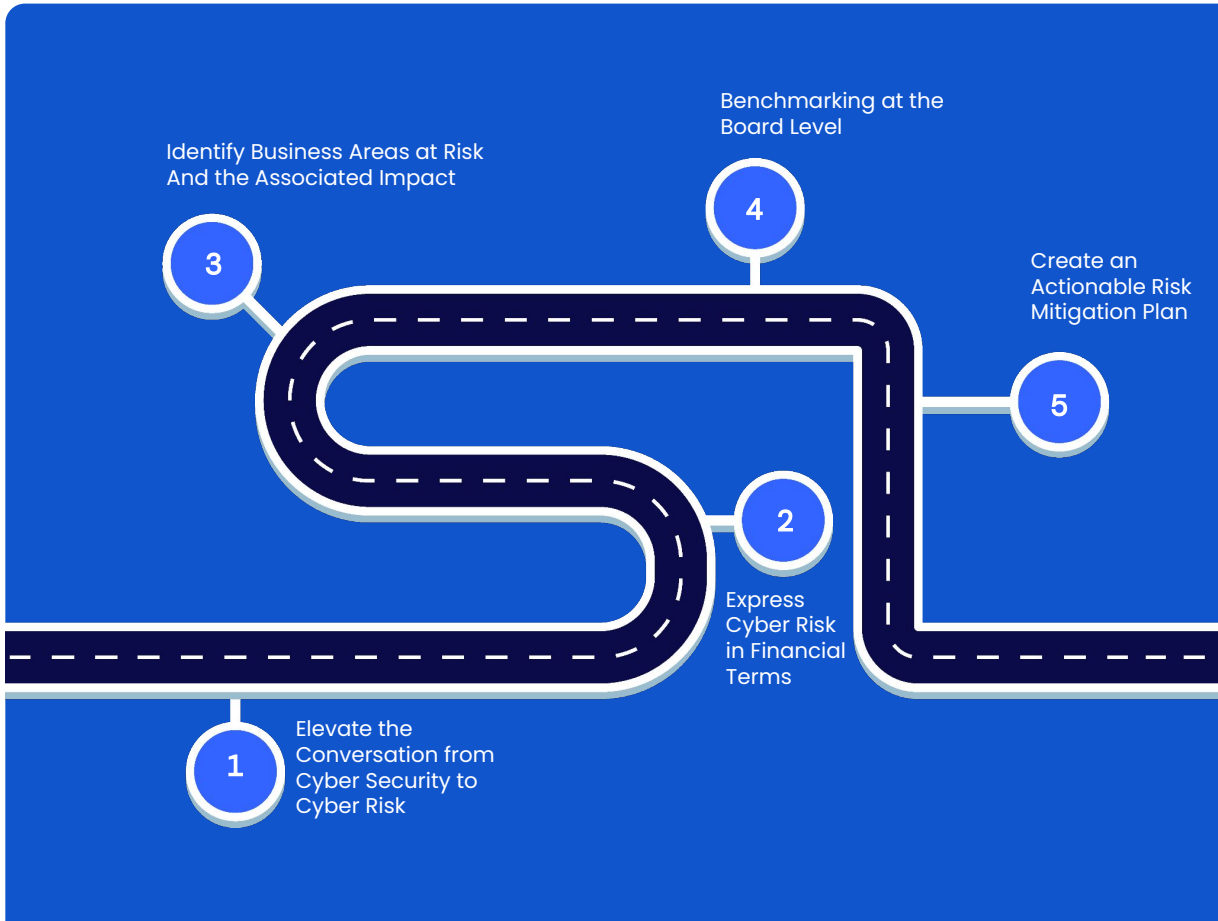
A Recipe for Success to Ace the Next Board Reporting

1. Elevate the Conversation From Cyber Security to Cyber Risk

CISOs need to reframe the conversation into one about risk, which is the language that the board understands. At the end of the day, the board has a fiduciary responsibility to protect the company from loss and understand how cybersecurity performance or risky vendors impacts that will enable them to make smart decisions and elevate the standing of security and risk leaders in their eyes.

PRO TIP 💡

- ❏ Elevate the conversation from cybersecurity to cyber risk, ensuring a focus on the actual on-network cybersecurity posture.
- ❏ Emphasize the criticality of aligning your cybersecurity program with key business areas at risk from cyber-attacks.



2. Express Cyber Risk in Financial Terms

Cyber risk is a form of business risk that can be expressed in financial terms. By considering factors such as revenue loss, mitigation costs, legal fees, increased customer turnover, and reputational damage, boards of directors can better understand the magnitude of cyber risk. The Board of Directors can more easily grasp cyber risk when it's quantified using financial metrics rather than abstract rankings such as high–medium–low.

PRO TIP 💡

- ❏ Evaluate potential revenue loss due to cyber incidents.
- ❏ Assess all the intrinsic as well as actual costs associated with a cyber incident, including potential legal expenses, regulatory fines, and litigation, the impact on customer turnover, examining the potential loss of trust.
- ❏ Understand the potential damage to the company's reputation and the associated financial consequences, such as decreased market share and brand devaluation.

3. Identify Business Areas at Risk and the Associated Impact

The single biggest responsibility of the board of directors is to protect the company and reduce risk. By pivoting your report away from a "bits and bytes" technology discussion and towards risk and risk that is specific or material to business objectives, you can empower the board to engage in a more meaningful discussion on cybersecurity. It is essential to identify key business areas vulnerable to cyber attacks and assist colleagues in comprehending how the cybersecurity program aligns with these risks. By clearly communicating how cyber risk will impact the business, you're more likely to get board engagement to create the right set of priorities and engage other executives to set the right strategies.

PRO TIP 💡

- ❏ Determine the key areas of the business vulnerable to cyber attacks.
- ❏ Aid colleagues in understanding the alignment of your cybersecurity program with this risk.

4. Benchmarking at the Board Level

The manual data collection process for board or Executive reporting can lead to inefficiencies, errors, and potential inconsistencies in the data presented to the board and executives. This process can also result in inaccuracies and mistakes that may affect the overall credibility of the information provided. Furthermore, these inaccuracies could adversely impact the board minutes,

PRO TIP 💡

- ❑ Establish benchmarks to compare your cybersecurity posture and breach risk with similar organizations.
- ❑ Provide recommendations to the board regarding the appropriate level of residual cyber risk for your organization.

5. Create an Actionable Risk Mitigation Plan

Your report should be supported by a comprehensive plan detailing how the organization's cybersecurity posture can be adjusted to reach the recommended level. Clearly explain the board's required support for executing this plan.

PRO TIP 💡

- ❑ Provide a comprehensive plan for changing the organization's cybersecurity posture to the recommended level.
- ❑ Clearly communicate the support required from the board to execute the plan.
- ❑ Continue monitoring and reporting the progress in reducing cyber risk over time.

How Effective Board Reporting Helps Your Business

How Effective Board Reporting Helps Your Business

Measurably Lower Overall Risk to Business

Organizations that effectively manage their cybersecurity risks experience a significant reduction in the overall risk to their business operations, minimizing the potential for substantial business loss or damage to brand equity.

Clear Understanding of Critical Risk Scenarios

Organizations can make well-informed business decisions with a very clear sight and understanding of critical risk scenarios. This enables them to navigate potential challenges with clarity and confidence.

Data-Backed Cybersecurity Budget Allocation

Equipped with data-backed insights and analysis, Chief Financial Officers (CFOs) can confidently allocate budgets for cybersecurity risk measures. This data-driven approach ensures that financial resources are appropriately allocated to address potential risks effectively.

High Confidence in the Cyber Risk Program & Leadership

The existence of a well-established security risk management program and strong leadership instills high confidence in the Board of Directors and the Chief Executive Officer (CEO). This confidence stems from the assurance that effective measures are in place to mitigate and manage security risks.

Proactive Breach Preparation and Response

In the event of a breach, the Board is not taken by shock, as expectation setting (aligning on residual risk) was done before a breach occurred. By proactively aligning expectations and having robust risk assessment processes in place, the Board can be well-prepared to handle a breach, avoiding the shock that may ensue. Discussing and aligning on residual risks beforehand allows for a more proactive approach to managing potential security incidents.

Safe Security Empowers Boardroom Excellence

How Safe Security Empowers Boardroom Excellence

The Safe Security platform delivers a data-driven, real-time solution for measuring, managing, and mitigating cyber risk. It arms CISOs with insights that help them understand top risks, express cyber risk in financial terms, help evaluate the adequacy of cybersecurity programs and budgets, define and approve risk appetite, and assess the impact of major cybersecurity initiatives – using defensible, standardized framework.

THE CYBER RISK CLOUD OF CLOUDS

1. **Ensures Security Measures are Aligned With Top Business Risks**
   With its AI-driven approach, Safe Security provides organizations with an aggregated view of enterprise security risk by bringing together multiple disparate cyber signals in a single place. This provides visibility across their attack surface, technology, people, and third parties, helping CISOs understand the top risks and answer questions such as *"What are our most important assets, and how are we protecting them?"*

   The SAFE Platform allows CISOs to evaluate their cyber controls' efficacy, mapped to the MITRE ATT&CK and D3FEND frameworks. Enterprise risk scenarios are scoped according to the MITRE ATT&CK Framework, which is continuously updated to help identify and measure the impact of emerging threats.

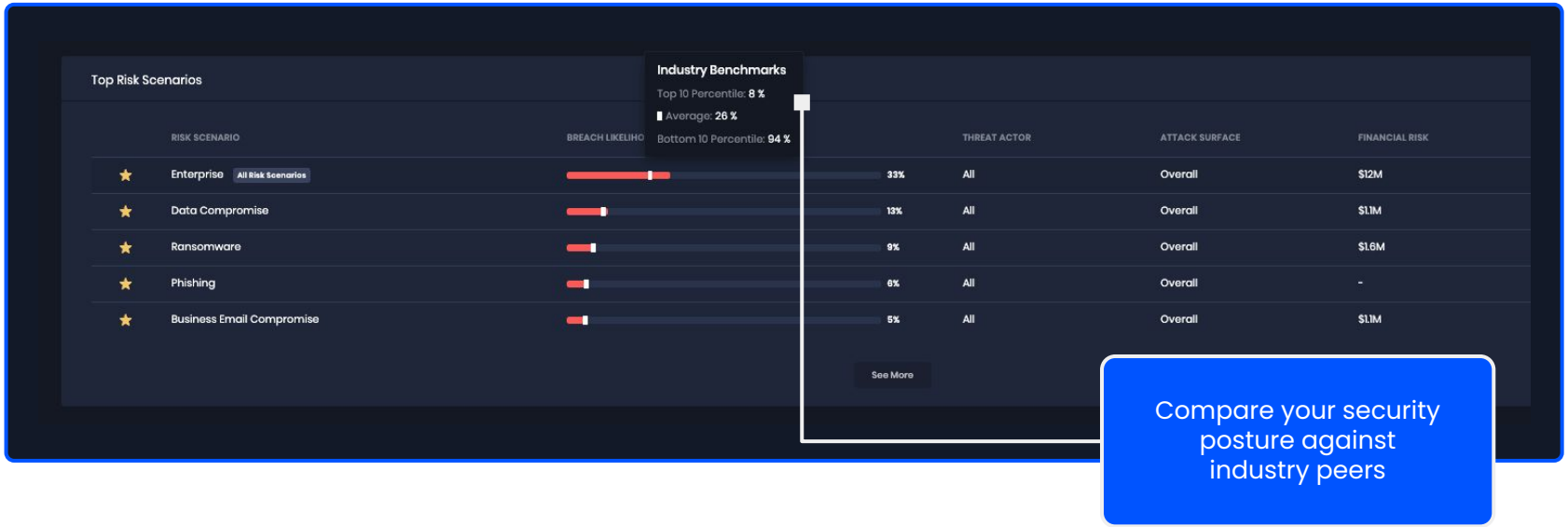
Top risk scenarios for your organization

See your breach likelihood for a risk scenario

Single Dashboard View of Your Enterprise-Wide Risk

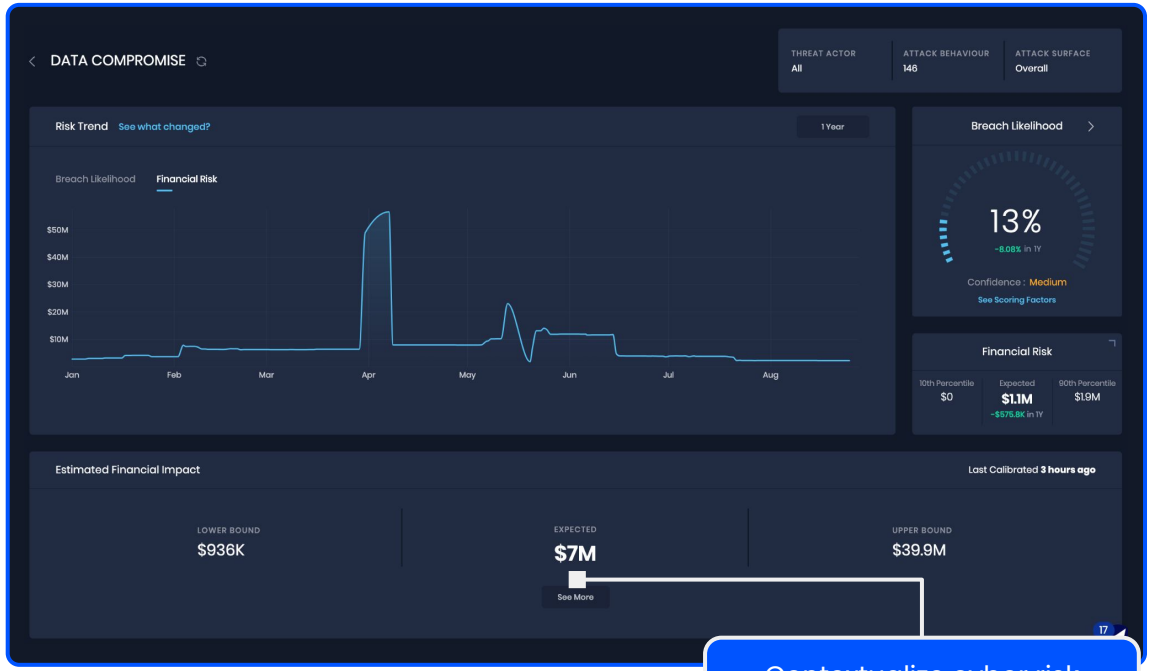
2. **Benchmark Against How You Are Positioned Against Your Peers in Your Industry**

   Safe allows you to benchmark your security posture – such as average, top 10 percentile, and bottom 10 percentile against comparable organizations in your industry. By doing so, you can gain insightful information to communicate your recommended cyber-risk goals to the board effectively. For instance, you can showcase the percentile of breach risk that your organization falls into and compare it to similar organizations in your industry for each risk scenario. This comprehensive analysis helps you provide a detailed understanding of your organization's security standing and helps support your recommendations.



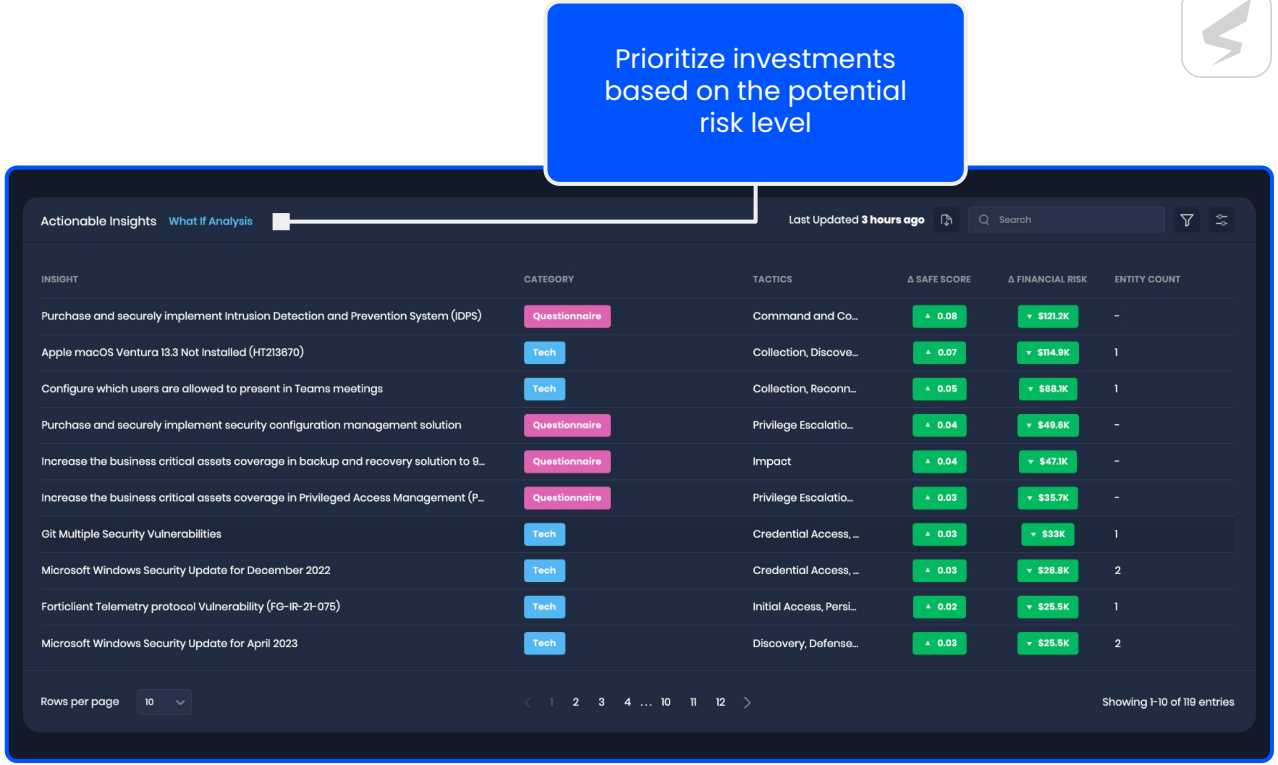
3. **Empower Your Board With a Defensible Dollar-Value Estimate of Your Financial Risk**

   Safe enables you to provide the board with a risk view with clear Breach likelihood and financial impact, enabling the board to understand the real cyber risk and focus on the risks that matter Safe uses an industry-leading framework such as the FAIR model, which provides a structured and quantitative way to communicate cybersecurity risks to management, the Audit Committee and the board. Internal audit can present audit findings clearly and meaningfully, including longitudinal trends and maturity improvements, after establishing a baseline for risk quantification.



Contextualize cyber risk as a business risk. See potential financial impact on the business from cyber risk

4. **Build an Actionable Plan to Show Your Program's Impact or Gaps With a Prioritized Mitigation Plan**
   Safe Security helps you prioritize security investments based on their potential risk level. By utilizing their services, you can identify the initiatives that will yield the greatest return on investment (ROI). Additionally, Safe Security enables the seamless integration of cybersecurity risk management into your overall enterprise risk strategy, ensuring comprehensive protection for your organization.



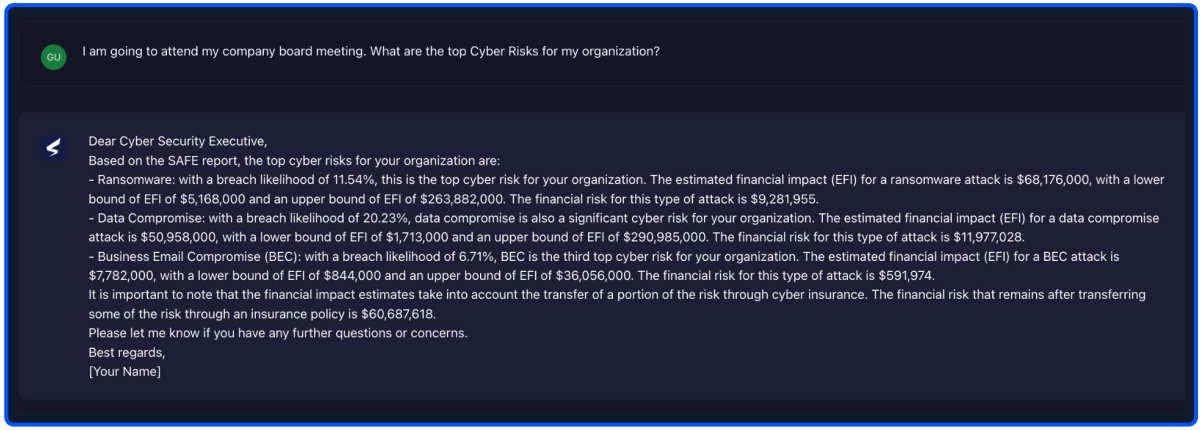
5. **Justify Current Cybersecurity Budget And Future Investment**

   The Safe Platform helps you to calculate the return on investment (ROI) for each cybersecurity investment. This makes it easy to justify the current cybersecurity budget and future investments. With this data, you can easily identify which investments are producing results and which investments are not, allowing CISOs to re-direct or adjust future cybersecurity investments accordingly.

Sample Board Report

6. Easily Communicate to the Board with AI-Enabled Chat and Dashboards

The SAFE Platform helps CISOs tell a compelling story to relevant stakeholders that clearly articulates the probable loss of exposure and the likelihood of an incident. Safe also provides actionable dashboards and reports to each risk owner with their security issues and risks. Safe visually displays trends over 90 days, 6 months, year-over-year, or any custom period. By delivering clear and consistent communication across stakeholders – including board members, audit committees, IT Risk committees, and insurers – you can ensure everyone is on the same page and understands their role in maintaining cybersecurity.



SafeGPT: Safe's Generative AI interface

SAFE's generative AI chat interface, SafeGPT, offers an intuitive platform for easily managing cyber risk, providing stakeholders with a clear and comprehensible overview of the organization's cybersecurity posture. With its user-friendly dashboard and natural language processing capabilities, SafeGPT enables users to ask targeted questions about their cyber risk data, determine the most effective strategies for mitigating risk, and respond confidently to inquiries from regulators and other key stakeholders.

The SAFE platform provides us with a much easier onboarding experience and objectively showcases the risk of business-critical applications and assets. I think cyber risk quantification platforms like SAFE will soon become a must-have for security/business leaders and board members for publicly traded companies.

Shaun Khalfan, CISO
Discover Financial Services

Build Credibility with Your Board on Cyber Risk Reporting With Safe Security

It is clear that effective cyber security risk management and board reporting can be a real challenge for any CISO.

The Safe Security Platform provides a comprehensive and dynamic solution for measuring, managing, and mitigating cyber risk. It empowers CISOs by providing valuable insights to comprehend top risks, express cyber risk in financial terms, evaluate the adequacy of cybersecurity programs and budgets, define and approve risk appetite, and assess the impact of major cybersecurity initiatives. This is achieved through a defensible and standardized framework, ensuring accurate and reliable results.

If you're interested in learning more about how to ace board reporting for your next meeting, schedule a demo with a cyber risk expert today.

RESEARCH SPONSOR

MITRE ATT&CK, TOP CONTRIBUTOR

PUBLISHER'S CHOICE AWARD RISK MANAGEMENT

GLOBAL INFOSEC AWARDS - RSAC 2023

BEST NEXT GEN CYBER INSURANCE PLATFORM

GLOBAL INFOSEC AWARDS - RSAC 2023

BEST RISK MANAGEMENT SOLUTION

CISO CHOICE AWARDS 2022™